AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY

Evaluating U.S. and Chinese Cyber Security Strategies Within a Cultural Framework

by

Diane E. Patton, Maj, USAFR
M.A., Management

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Wing Commander Graem Corfield, RAF

Maxwell Air Force Base, Alabama

April 2016

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Abstract

With the 2015 release of both an updated United States Department of Defense Cyber Strategy and a Chinese Ministry of National Defense white paper on military strategy, these public documents regarding States' use of cyber technology and objectives for national security offer an insight into deeper military strategy for future security concerns. It is possible to examine the underlying objectives within these strategies to develop a theme for an organization's behavior in the cyber domain. Strategy is shaped by broad cultural dimensions, and this paper discusses two of the existing cultural dimensions theories and proposes three additional dimensions to provide context for organizational and military strategy. Although phrasing this discussion within a State-to-State construct here, it should be noted that strategic culture is not limited to nation-states. Highlighting the variance in cultural dimensions which frame anticipated actions and response sets provides an ability to construct a flexible military response to both state and non-state actors. Therefore, evaluating these individual themes within a cultural framework and how organizations view security in general, provides a broad view of how culture shapes strategy and doctrine, and provides a basis for discussion regarding the flexibility for the United States military to respond to cyber threats across a broad spectrum.

Cultural Context: What is Culture?

Jiyul Kim, Director of Asian Studies and Coordinator for Regional Studies at the Army War College, believes that the US Department of Defense (DOD) is in the midst of a "cultural turn,"[1] essentially a renaissance bringing about a new appreciation for culture and its influence on national policy and strategy. Culture implies a look-back, a context from which to understand how and why groups of people vary in their interactions with each other and the world around them. Cultural influences are evident at the organizational, national, and strategic levels. Common themes, however, are that culture is shared, transmitted, malleable, and internalized by a common group of people or a society. In terms of organizational culture, Schein defines this is as "a pattern of shared basic assumptions learned by a group as it solved its problems of external adaptation and internal integration"[2] which are discernable as observed behaviors, or artifacts, stated beliefs, goals, and values, and basic underlying assumptions.[3]

In 2002, Jeffrey Lantis compiled a large body of theory on strategic culture, especially as relating to state strategy and policy formation, and states that the theory of strategic culture has evolved in recent years to "explain national security policy"[4] and the influence on state behavior. Of particular note is Jack Snyder's foundational work on strategic culture to interpret military strategy. Snyder's definition of strategic culture is "the sum total of ideas, conditioned emotional responses, and patterns of habitual behavior,"[5] yet limits this culture as belonging to a national institution. Key elements of Snyder's strategic culture rely on "the context associated with perceived security threats and technological development … attitudes and beliefs … [and] the role of the military…"[6] in formulating strategic decisions.

Social psychologist Geert Hofstede defined culture as "collective programming of the mind,"[7] and had conducted comprehensive studies on national culture, originally devising four

(now six) cultural dimensions which distinguish the members of one group from the members of another. Hofstede's work provides a quantifiable manner in which to compare cultural influences from the national and regional scale, using a 1-100 scale as a values continuum. Although this is alone is not a determinant of specific behaviors, such cultural dimensions are useful in shaping predictable courses of action that an organization would take.

Hofstede's National Cultural Dimensions

Starting with Hofstede's work as a foundation to introducing a cultural framework, the six dimensions he proposes are:[8]

1. Power Distance: How power is distributed within a society and the degree to which human inequality is tolerated. High scores in this dimension indicate that power and authority are inherent, with inequality understood and tolerated; low scores indicate societies that value cooperation and have less tolerance for societal hierarchies.
2. Individualism/Collectivism: The degree to which people prefer joining groups; high scores indicate an individualistic nature of society, emphasizing self-pursuits, while low scores demonstrate the desire for a tightly-knit social framework, with the goals of the group more important than those of the individual.
3. Masculinity/Femininity: A high score ("masculine") represents the values of achievement, assertiveness, and materialism within a society, while a low score ("feminine") represents a preference for cooperation, modesty, and values relationships and quality of life.
4. Uncertainty Avoidance: The degree to which members of a society are comfortable with ambiguity and unstructured circumstances; high scores in this index represent societies that maintain and honor tradition, while valuing rules and work ethic, while low score societies are more tolerant of new ideas and innovation, are willing to take more risks, and value trust.

5. Long Term/Short Term Orientation:[9] High scores in this dimension demonstrates a culture's long-term view of time through a pragmatic nature and encouraging modern and innovative approaches; low scores reflect a culture that values time-honored traditions and views change with suspicion, tending to be more short-term thinkers.
6. Indulgence/Restraint:[10] A high score ("indulgent") represents a culture that tends to focus more on individual happiness, freedom, and leisure activities. In contrast, a low score ("restrained") indicates societies that devalue personal gratification and impose a greater number of societal norms.

When considered holistically, these cultural dimensions provide a context for how and why societies and organizations think, act, and reflect on their behavior. Combined with Kim's broader cultural dimensions theory, as well as the proposed strategic culture dimensions, strategic direction is devised based on shared cultural beliefs.

Kim's Cultural Dimensions

In a similar manner, Jiyul Kim argues that the Analytical Cultural Framework for Strategy and Policy (ACFSP) is a way to view the world through a comprehensive lens, and provides three cultural dimensions for political and strategic values and interests. The three dimensions he proposes are *identity*, comprised of both individual/biological and socially-derived traits, which has the "power to mobilize the collective towards a common purpose;"[11] *political culture*, which is the communal set of values, traditions and expectations of a society, which gives rise to a political system and its strategic culture;[12] and lastly *resiliency*, which reflects the adaptability of a culture to external forces.[13] Kim does not attribute any particular dimension with a continuum, merely noting that the ACFSP is a "systematic and analytical tool for exploring the cultural aspects of the political and strategic landscape,"[14] however his work

has applicability to the idea of strategic culture that Snyder describes, and provides another frame of reference for cultural analysis of strategy and policy.

Proposed Strategic Cultural Dimensions

The proposed strategic cultural dimensions below are meant to be viewed as a continuum, as opposed to binary concepts, which are applicable to the development and execution of organizational strategy and doctrine. These concepts were developed as a result of examining national strategy documents, and research in the field of organizational development, and encompass a global look at how organizations form strategy to pursue their interests and goals.

1. Value of Information (Information-oriented vs. Task/Mission-oriented): This dimension captures the degree to which information, data and wisdom is valued. The effect of this can be realized in the continuum between inaction vs. action, defense vs. offense, but neither analogy is as accurate as capturing the idea that information, rather than activity, is the primary driver of strategy.
2. Value of Technology/Innovation (Technology vs. Tradition): This dimension is the valuation of technology over tradition and historical legacies. It is a measure of innovation, creative thinking and reliance on scientific advances.
3. Value of Security (Secrecy vs. Openness): This dimension captures the degree to which security is valued within an organization. High security values correspond with secrecy, denial of access, and a protection of information. Low values indicate openness, accessibility, and a tendency towards disclosure of information.[15]

Summary on Culture

Hofstede's work is, by definition, nationally-focused, though important relationships can be drawn by combining and comparing cultures within a regional construct to generate a general

view of regional cultural influences. Kim's analytical framework notes that the most traditional source of identity has been the nation-state and influence of nationalism, but makes allowances for trans-national, sub-national (i.e. tribal), and regional collective identities that have potent political force.[16] The resultant political culture which evolves from the identity of the group therefore determines interests, policy and strategy of its constituents. Resilience, therefore, is the ability of the group to resist, adapt to, or embrace change as a result of globalization and other external factors. The proposed strategic cultural dimensions are meant to be viewed as a continuum, similar to Hofstede's, but are not tied to regional or national borders, and can be applied to any state or non-state actor that generates strategy based on its accepted cultural influences. When combined with Hofstede's dimensions, and Kim's framework, strategic vision and goals may start to become more predictable to an outside observer.

Using the originating geographical region/nation of a non-state actor, Hofstede's cultural dimensions may provide useful data on expected strategic drivers for that group. However, in the case of transnational organizations, Hofstede's analysis becomes less applicable. In these instances, Kim's analytical cultural framework, as well as the proposed cultural dimensions of strategy above, will yield a deeper insight into predicted group or organizational strategy and expected courses of action. More importantly, cultural influences can preclude the ability of any organization to fully express and realize strategic goals, and such influences will limit the options of military doctrine to that which satisfies the organization's cultural constraints.

Highlights of National Cultures: United States

The United States, as categorized by Hofstede's dimensions are: Low Power Distance (realized under democratic principles), Individualistic, Masculine, Moderate Uncertainty Avoidance (which indicates a fair degree of acceptance of new ideas and willingness to try new

things), Short-Term oriented, and Indulgent.[17] Kim contends that the US identity is closely tied with place, over inherited privilege; this, combined with capitalism and a pioneering spirit, has given rise to the US as an innovative, adaptive, highly resilient society with a complex political landscape.[18] In his definition of resilience, this may be the case, yet Hofstede's analysis disagrees, finding that the US is less innovative than comparative nations, and is less adaptive and accepting of change than initial glance may suggest. The complexity of the political culture may further serve to constrain action, especially from the proactive standpoint, while imbuing national strategy with excessive reliance on short-term, offensive measures. From a strategic culture standpoint, based on Hofstede's uncertainty avoidance and masculinity dimensions, and evident in the stated strategy of the United States,[19] the US is task-oriented, placing a high value on goals and measures. Information turnover is considerably high, and a reliance on historical lessons on strategy is scant in developing doctrine, especially considering the cyber domain. SAASS scholar Todd Zachary finds, "the cultural values connected with effort and activity add to the American belief that 'it is better to do something than to sit back and do nothing.'"[20] The US highly values technology, innovation, and individual initiatives, and embraces scientific advancement to secure national interests. This emphasis on technology over tradition is founded on both the short-term orientation of national culture, as well as the political ideology of the US; liberal, free-market, and educated democracies tend to adopt and embrace technology.[21] Furthermore, the US tends to demonstrate a high value on information openness, as compared to security. From an infrastructure standpoint, US information systems were designed on the basis of trust and freedom of communication, while incorporating a high degree of network resilience, which has led to the retroactive application of security measures, with little incentive or emphasis on such protective practices.

Highlights of National Cultures: China

In contrast, China's cultural analysis shows: High Power Distance, Collectivist, Masculine, Low Uncertainty Avoidance (meaning comfortable with ambiguity and adaptable to new situations), Long-Term oriented, and Restrained.[22] Kim's work does not specifically examine Chinese culture, but notes that Eastern nationalism, as well as the heavy influence of historical writings, and East Asian/Confucianism collectivist nature is an important part of defining identity.[23] Alistair Iain Johnson notes, "China has exhibited a tendency for the controlled, politically driven defensive and minimalistic use of force that is deeply rooted in the statecraft of ancient strategists."[24]

Li Bingyan, a retired Major General of China's People's Liberation Army (PLA), has written extensively on Chinese strategy. He notes that, "Westerners focus on technology while Easterners focus on strategy," tending to focus efforts on a singular issue, rather than a comprehensive solution, and that the West tends to rely on force, rather than coordinating intellect and strength.[25] This concept of harmony between information and weaponry is reflected in Chinese writings on integrating technology with strategy.[26] Another view from the PLA is seen in the work of Zhang Xiaojun and Xu Jia, who compare the differences between Chinese and US strategic culture, noting that China has typically been peace-oriented and driven by morality, as compared to US nationalistic and economic drivers.[27] While this view is heavily biased, it is worth noting their analysis of Chinese culture in warfare studies. They find that Chinese convention "respects inaction"[28] and the teachings of Sun Tzu, thus favoring the tradition over technology aspect of strategic culture. They also believe that China's military strategy should be defensively-oriented, especially when considering the asymmetric warfare advantage that the Chinese value; that is, that "victory [should be] gained from knowledge, not

strength."[29] They contend that the US emphasizes competition, strength, and the application of force,[30] which supports the analysis of US as task-oriented, compared to information-oriented. While Chinese writings may indeed be prejudicial towards the US and ignore their own recent expansionist actions across the globe, they are worth examining for their influence of strategic and national culture,[31] and how their measures within the cultural dimensions can shape predicted courses of action for the future.

Applications to Respective Cyber Strategies and National Security

Comparing the two cultures, both nations demonstrate a proclivity towards Masculine values, with China slightly higher on the scale than the US. Both societies are therefore success-oriented, driven, and adhere to the idea of "service before self," to borrow an aphorism from the US Air Force. As such, this dimension influences both states to develop cyber strategies and forces, to maintain the "tip of the spear" edge in information technology advances. This, however, is where the similarities between the two national and strategic cultures end.

The dimension of openness builds on psychology and trait theory, and figures strongly into the strategic culture of a particular organization. Cultures that are more open are "more willing to entertain novel ideas and unconventional values."[32] East Asian cultures, who are traditionally more collectivist in orientation, therefore should demonstrate lower openness rankings in this dimension. Openness factors into adoption of technology and incorporation of innovation into strategic thought. In 2010, Chinese analysts had come to the conclusion that "the country remained [merely] an imitator of technical innovation… and had not provided the enabling environment"[33] that their competitors had, stifling true technological cultural change. As recently as 2013, this analysis is still highly relevant; the basis of current Chinese weapons platforms in most domains (air, land, missile, space) is heavily dependent on foreign intelligence,

both licit and illicit.[34] However, China held a rich history of innovation prior to the modern age;[35] this may prove to become stronger, if their weak industrial complex is transformed along with the informatization of national society.

The basis of China's military strategy is such *informatization*, the transformation from a traditional, mechanized force, to an information-based one, mirroring the goal of expansion of the information society within China itself. China's strategic culture is heavily influenced towards the valuation of information in the first proposed cultural dimension. Information flow is heavily controlled by the government, and is a function of the high power distance evident in Chinese national culture. Therefore, any claims that "rogue" individuals or groups are behind cyberattacks can be viewed with suspicion; it is more likely that such actions were directed and supported by the government itself. While this may be useful in determining a counter-strategy towards the Chinese state, plausible deniability of attribution siphons attention away from formulating a US or international course of action.

Indeed, the concept of security is heavily touted in current Chinese military strategy: "Therefore, it is necessary to uphold a holistic view of national security, balance internal and external security, homeland and citizen security, traditional and non-traditional security, subsistence and development security, and China's own security and the common security of the world."[36] Security sentiment is seen in the information network infrastructure itself, from "the Great Firewall" and internet censorship to the security monitoring/public surveillance program instituted under the Golden Shield project.

Chinese history and culture in war focuses heavily on deception, camouflage, and "seeking out strategic advantage."[37] Today, camouflage is broadened into a concept that includes degradation of enemy weapons systems, communications and control nodes, and information

systems, while protecting the integrity and capabilities of their own systems, using the full range of electromagnetic spectrum tools of modern technology.[38] Camouflage becomes part of the strategic process that is developed by the Chinese government, facilitated through the cyber spectrum, and extends through operations at all levels throughout the entire course of a conflict.[39] This idea is strongly influenced by China's valuation of secrecy/security; through "strategic ambiguity"[40] such as hiding strategic objectives, gathering and controlling information, and using this to manipulate enemy perceptions and activities, the state will be successful in achieving military victory.

Their view of asymmetric warfare, as applicable to cyber is evident in PLA Major Peng Hongqi's 2004 military writings, that "an inferior force must conduct information reconnaissance and prepare confrontational responses as asymmetric checks and balances."[41] PLA strategy and doctrine since the inception of informatization has largely prepared the military "to prosecute short, high intensity campaigns, employ advanced technology… [and] level the technological playing field"[42] against a stronger military adversary. Therefore, China's military objective is gathering as much of the enemy's information as possible, while hiding and protecting their own information through information secrecy. Due to their comfort in future uncertainties, and in line with their long-term orientation and information-focused traditions in warfare, it should come as no surprise that China relies heavily on espionage activities, both traditionally and in the digital realm.

Innovation and informatization, according to the PLA, are critical to victory in the cyber realm. This should be practiced and refined throughout peacetime and employed in battle. Furthermore, the Chinese realize that deception and stratagems may no longer suffice in the information age; tactics must be combined with technology to "enable the optimum level of

combat efficiency."[43] This proves a large obstacle for Chinese strategic culture to overcome; to promote and embrace technology in equal status to tradition, and bring about short-term objectives into strategic decisions due to the rapid pace of technological advances. Perhaps the increase in cyber intrusions on global sites over the last decade, attributed to Chinese actors, is one point of evidence towards such cultural change in Chinese strategic thought. Li Yuxiao and Xu Lu write that China lacks personnel who can contend with the inherent openness and flexibility of the internet, ultimately leading to degradation in cyber security on a national level.[44] Further, the widespread influence of internet access has changed perceptions on how open the political process in China should become, and the government is adapting to this call for transparency.

While the US values openness in information distribution and the underlying system architecture is based on this principle, US affairs in information operations have been less transparent. Reports of US espionage activities, released in 2013, contradict the value of openness that the national culture identifies with. Further, international observers view the "naming and shaming" of adversarial activities in cyberspace as hypocritical, and contraindicated to US goals of cooperation and norm-building. Such "shaming" may also undermine diplomatic relationships,[45] most notably in China, but evident in cultures that hold public opinion in high regard.

The US views itself in terms of strength, seen in its masculine and indulgent dimensions; asymmetric warfare is for the weak.[46] Strategist Colin Gray agrees that the US strategy focuses on symmetrical, conventional enemies, rather than an asymmetrical one.[47] In addition, the US has historically prepared for a war of attrition, a view of mass over maneuver, long-held by US military strategists.[48] The 2015 National Military Strategy further makes the distinction on the

use of military force between responding to a state threat and a non-state threat, emphasizes the importance of addressing state actors, and notes that future conflicts are more likely to be prolonged in nature.[49]Alexander Vacca foresees a US Defense Department cyber security model building upon lessons learned from airpower theorists;[50] if this holds true, as is certainly apparent in the latest DOD Cyber Strategy, it is fatally flawed. Reliance on moral effect has been shown to be inconsequential in kinetic strikes, presumably one of the objectives of a cyber strike, and the network effects of cyberspace negate moral effect due to system redundancies.

Lastly, rests the US's apparent overreliance on technology. "The US military's heavy dependence on technology makes it uniquely vulnerable to an adversary who can neutralize its advanced systems."[51] This emphasis on technology is not limited to the military, but it is reflected most acutely in discussions on national strategy, military equipment acquisition, and development of weapons platforms. Although the social culture may be accepting of technological advances, this has not yet translated into an effective way for the US military to employ such innovation. The 2015 DOD Cyber Strategy goal of training a cyber workforce, building technical capabilities, and assessing the readiness of a cyber mission force is a step towards methodically improving cyber and information awareness into military doctrine.

The combination of an information-deficient, technologically-dependent, and short-term oriented political and military strategy focused on an outdated threat model is not an effective way to address current and future combinations of operations in cyberspace. On the converse, an information-rich, innovation-deficient, overly cautious mindset is causing an equal stagnation of strategy. The rhetoric requires a middle ground to propel strategy into actionable activities, and it must be palatable for the underlying national and strategic culture to implement.

Broad Implications for Future Strategy

Secrecy is inherent in authoritarian-type governments, where the government must keep broader control over information in order to remain in power; in converse, democracies rely on openness, and secret-keeping and intrusive security measures undermine democratic principles.[52] Therefore, while the US relies on information openness as an extension of its political democracy, it is now finding difficulties in developing and implementing strong security measures in cyberspace. On the one hand, such openness can help, as articulated in the 2011 US International Strategy for Cyberspace, through nurturing innovation, and valuing research and development to enrich society.[53] The Strategy further states that stifling free information flow hampers international effectiveness, and provides only the "illusion of security,"[54] alluding to China's repressive firewall. Yet, trust comes with a price: an organization must provide network defense and security for its end users, which contributes to the accuracy of information, reliability of service, and freedom from malicious code. Security is seen as a uniting feature of Chinese ideology; it is provided by the government, for the people, to maintain a freedom from external interference. This idea of security, privacy, and personal freedom is more closely aligned to a European view of security, in contrast to the US view, which more closely relates to the idea of personal freedom to operate without government obstruction.

As a corollary to the security/openness dimension proposal, authoritarian organizations are generally slower to adopt technology, and tend to place greater controls over technology.[55] This poses a challenge to those groups and states, such as China, who seek to bring information operations/warfare into their strategy, since it is antithetical to their culture to embrace and employ technology. However, as Corrales and Westhoff argue, relative wealth, indicative of per capita GDP, tends to overcome authoritarian restrictions on internet availability;[56] this effect is

seen markedly in China's population, which has enjoyed greater internet usage as their per capita GDP has continued to rise. Furthermore, China has brought its opinions to the table more often in international cooperative efforts, especially in relation to cyber norms and laws over the last decade, which could relate to their improved economic standing and willingness to negotiate within the bounds of their security-minded model.

Just as China is evolving its cyber norms to meet the globalized world, the US is slowly shifting its strategy towards international cooperation as well. For example, the way its military cyber command, USCYBERCOM, is organized, intelligence operations often win out over "action-minded" military operations. Long-term, information-gathering opportunities may provide a new direction for US strategy, shifting from short-term reactive actions, to long-term, broader grand strategy. Cooperative diplomatic efforts towards targeting transnational criminal activities, such as the recent US-China Cyber agreement, may also change the view of US strategists towards addressing a broader range of actors within cyberspace.

The bureaucratic properties of any state government will affect the implementation of strategy. Non-state actors are predictably more agile, and can utilize the inherent decentralization of cyberspace more effectively. Thus, it would be wise for the US to focus more attention on asymmetric threat strategies to predict and plan for future cyber attacks from both expected and unexpected actors. To deter such attacks, the specific threat itself does not matter;[57] by interrupting the opportunity to attack, or reducing the impact/criticality of a system's vulnerability, the deterrence formula is changed to the US advantage,[58] while maintaining the current state of secrecy surrounding offensive cyber capabilities.

Although the above discussion has been focused on two state actors, as represented as the most critical threat on the cyber actor continuum,[59] the rapid spread of global communication

networks, interconnected economies, and easy access to technology has all given non-state actors the ability to act independently, legitimately, and with greater power. "Nonstate actors now have capabilities once only available to states – to influence populations, provide governance services, organize transnational social and economic networks, and raise funds and gather resources from across the globe."[60] Strategic culture is not tied to a nation-state; the influence of global interconnectedness and communications transcends geopolitical boundaries. Non-state actors, such as transnational crime groups, terrorist organizations, and political proxies often articulate their own group's strategy. Dan Drezner argues that while non-state actors can certainly act alone, they have effects on the parent state;[61] taking this one step further, it does not matter whether a cyber actor is a state or not, all actions should be prosecuted in the same manner, Moreover, Andrew Cutts states, the tendency is for threats (risk) to increase over time,[62] further marking the importance of acknowledging the non-state threat to national security.

Conclusion

The current literature on cyber strategies has been lacking a cultural analysis to determine the trajectory of an organization or state's intended goals in the cyber domain. Analyzing the US and China public military cyber language has demonstrated how culture has influenced the process of formulating strategy and doctrine. In addition, determining areas where strategy's rhetoric may run contrary to its organization's underlying culture, through evaluating the existing and proposed cultural dimensions models, allows for strategists to develop avenues to cooperate (or exploit) in response. The US should factor these considerations into its future cyber strategy to address the wide range of threats, regardless of intent, to strengthen overall national security and refine military strategy to reflect a move towards long-term information-based operations.

Bibliography

Ehsan Ahrari. "Transformation of America's Military and Asymmetric War." *Comparative Strategy* 29, no. 3 (2010): 223-244. doi: 10.1080/01495933.2010.492191

Austin, Greg. *Cyber Policy in China*. Cambridge, UK: Polity Press, 2014.

Butler, J. Corey. "Personality and Emotional Correlates of Right-Wing Authoritarianism." *Social Behavior and Personality* 28, no. 1 (2000): 1-14. doi: 10.2224/sbp.2000.28.1.1

Corrales, Javier and Frank Westhoff. "Information Technology Adoption and Political Regimes." *International Studies Quarterly* 50, no. 4 (December 2006): 911-933. http://www.jstor.org/stable/4092785.

Cutts, Andrew. *Warfare and the Continuum of Cyber Risks: A Policy Perspective*. Washington, DC: Department of Homeland Security, 2009. https://ccdcoe.org/publications/virtualbattlefield/04_CUTTS_national%20cyber%20risk%20v2.pdf

Department of Defense. *The DoD Cyber Strategy*. Washington, DC: Office of the Secretary of Defense, 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Drezner, Daniel W. "Global Governance: Bringing the State Back In." *The Academy of Political Science* 119, no 3 (Fall, 2004): 477-498. http://www.jstor.org/stable/20202392

Gowder, Paul. "Secrecy as mystification of power: Meaning and ethics in the security state." *I/S-A Journal of Law and Policy for the Information Society* 2 (2005): 1-25. http://www.is-journal.org/V02I01/2ISJLP001.pdf

Hofstede, Geert. *Cultures Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations*, 2nd ed. Thousand Oaks, CA: Sage Publications, 2001.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, DC: The White House, 2011.

Johnston, Alastair Iain. *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. Princeton, NJ: Princeton University Press, 1995.

Joint Publication (JP) 3-12 (R). *Cyberspace Operations*. 5 Feb 2013.

Kim, Jiyul. "Cultural Dimensions of Strategy and Policy." Letort Paper. *Strategic Studies Institute*. Army War College. May 2009.

Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Prepared for the U.S.-China Economic and Security Review Commission, Northrup Grumman Corp. 7 March 2012.

Lantis, Jeffrey S. Lantis. "Strategic Culture and National Security Policy." *International Studies Review* 4, no. 3 (Autumn, 2002): 87-113. http://www.jstor.org/stable/3186465.

Lindsey, Jon. R., Tai Ming Cheung, and Derek S. Reveron. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York. Oxford University Press, 2015.

Luke, Bryan. "Recognizing and Adapting to Unrestricted Warfare Practices by China." Master's thesis: Air War College, Air University (2012). http://dtlweb.au.af.mil/webclient/DeliveryManager?pid=57093.

Ministry of National Defense. *China's Military Strategy*. White Paper. Beijing: The State Council Information Office of the People's Republic of China, 2015. http://eng.mod.gov.cn/Database/WhitePapers/index.htm.

The National Military Strategy of the United States of America. Washington, D.C. June 2015.

Pion-Berlin, David and Harold Trinkunas. "Latin America's Growing Security Gap." *Journal of Democracy* 22, no. 1 (January 2011): 39-53. http://search.proquest.com/docview/854323300?accountid=4332

Schmidt, Andreas. *Secrecy Versus Openness: Internet Security and the Limits of Open Source and Peer Production.* The Netherlands: Uitgeverji BOXPress, 2014. doi:10.4233/uuid:ecf237ed-7131-4455-917f-11e55e03df0d.

Schmitt, David P., Jüri Allik, Robert R. McCrae, Verónica Benet-Martínez. "The Geographic Distribution of Big Five Personality Traits: Patterns and Profiles of Human Self-Description Across 56 Nations." *Journal of Cross-Cultural Psychology* 38, no. 2 (March 2007): 173-212.

Schein, Edgar H. *Organizational Culture and Leadership*, 3rd ed. San Francisco, CA: Jossey-Bass, 2004.

Snyder, Jack L. *The Soviet Strategic Culture: Implications for Nuclear Options*. RAND Report R-2154-AF (Santa Monica, CA: RAND Corporation, 1977).

Thomas, Timothy L. *The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force.* Fort Leavenworth, KS: Foreign Military Studies Office, 2009.

Wooten, Kevin B. "Chinese National Security Strategy: Implications for a 21st Century Air Force." Master's thesis: Air War College, Air University (2005). http://dtlweb.au.af.mil/webclient/DeliveryManager?pid=36962

Zachary, Todd M. "Wearing the White Hat: The Effect of American Strategic Culture on Implementing National Strategy." Master's thesis: School of Advanced Airpower Studies, Air University (2000). http://dtlweb.au.af.mil/webclient/DeliveryManager?pid=42977.

Endnotes

1. Kim, *Cultural Dimensions*, 2.
2. Schein, *Organizational Culture and Leadership*, 17
3. Ibid., 26
4. Lantis, *Strategic Culture*, 87
5. Snyder, *Soviet Strategic Culture*, 8.
6. Lantis, *Strategic Culture*, 94
7. Hofstede, *Culture's Consequences*, 1.
8. Ibid., 79-81, 145-147, 209-213, 279-280 351-354
9. This cultural dimension was added to the model in 2001 as a result of the Chinese Value Survey in 1985.
10. This cultural dimension was added in 2010 after further studies on the concept of happiness and results through the World Values Survey.
11. Kim, *Cultural Dimensions*, 17.
12. Ibid., 20-21.
13. Ibid., 23.
14. Ibid., 3.
15. Schmidt, *Secrecy Versus Openness*, 55.
16. Kim, *Cultural Dimensions*, 19.
17. Hofstede website scoring model for United States: Power Distance = 40, Individualism = 91, Masculinity = 62, Uncertainty Avoidance = 46, Long Term Orientation = 26, Indulgence = 68, http://geert-hofstede.com/united-states.html
18. Kim, *Cultural Dimensions*, 12.
19. See the United States 2015 National Military Strategy, 2015 National Security Strategy, 2015 DOD Cyber Strategy
20. Zachary, "Effect of American Strategic Culture," 47.
21. Corrales and Westhoff, "Information Technology Adoption," 912.
22. Hofstede website scoring model for China: Power Distance = 80, Individualism = 20, Masculinity = 66, Uncertainty Avoidance = 30, Long Term Orientation = 87, Indulgence = 24, http://geert-hofstede.com/china.html
23. Kim, *Cultural Dimensions*, 43-44.
24. Johnson, *Cultural Realism*, 1
25. Li Bingyan, "Emphasis on Strategy: Demonstrating the Culture of Eastern Military Studies," China Military Science, 2002, no. 5, in Thomas, *Dragon's Quantum Leap*, 66.
26. Lin Ronglin and Cui Tao, "Innovation in Chinese Military Thinking Through Comparison with the West," China Military Science, 2006, no. 5, in Thomas, *Dragon's Quantum Leap*, 67.
27. Thomas, *Dragon's Quantum Leap*, 76.
28. Ibid.
29. Ibid., 77.
30. Ibid.
31. Ibid., 79-80.
32. Schmitt, et al., "Big Five Traits," 205.
33. Austin, *Cyber Policy in China*, 110. See also Krekel, et al., *Occupying the Information High Ground*, 22 and Thomas, *Dragon's Quantum Leap* for historical points of reference.
34. Jon Lindsey and Tai Ming Cheung, in Lindsey, et al., *China and Cybersecurity*, 68-70.

35. Wooten, "Chinese National Security Strategy," 25.
36. China's Military Strategy, section II.
37. Thomas, *Dragon's Quantum Leap*, 1.
38. Ibid., 96.
39. Ibid., 99.
40. Wooten, "Chinese National Security Strategy," 2.
41. Peng Hongqui, "A Brief Discussion of Using the Weak to Defeat the Strong under Informatized Conditions," Beijing Zhongguo Junshi Kexue (China Military Science), 2008, no. 1, in Thomas, *Dragon's Quantum Leap*, p. 42.
42. Krekel, et al., *Occupying the Information High Ground*, 15.
43. Thomas, *Dragon's Quantum Leap*, 114.
44. Li Yuxiao and Xu Lu, in Lindsey, et al., *China and Cybersecurity*, 231.
45. Fred H. Cate, in Lindsey, et al., *China and Cybersecurity*, 324.
46. Ahrari, "America's Military and Asymmetric War," 224.
47. Luke, "Unrestricted Warfare Practices," 4.
48. Zachary, "Effect of American Strategic Culture," 42-43.
49. *National Military Strategy 2015*, i.
50. Vacca, "Military Culture and Cyber Security."
51. Sharp, "Over-Promising and Under-Delivering," 983.
52. Schmidt, *Secrecy vs. Openness*, 57. See also Gowder, *Secrecy as a Mystification of Power* and Butler, *Right-Wing Authoritarianism*.
53. International Strategy for Cyberspace, 3.
54. Ibid., 5.
55. Corrales and Westhoff, "Information Technology Adoption," 917.
56. Ibid., 918.
57. Air Command and Staff College, Cyber Operations seminar, 30 September 2015, Maxwell AFB, AL.
58. Air Command and Staff College, Cyber Operations seminar, 2 October 2015, Maxwell AFB, AL.
59. Cutts, "Continuum of Cyber Risks," 3-4. See also JP 3-12, *Cyberspace Operations*, I-6-I-7.
60. Pion-Berlin and Trinkunas, "Latin America's Security Gap," 41.
61. Drezner, "Global Governance."
62. Cutts, "Continuum of Cyber Risks," 4.